REMARKS

The present Amendment amends claims 1-7. Therefore, the present application has pending claims 1-7.

35 U.S.C. §102 Rejections

Claims 1-7 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,917,615 to Reifman, et al. ("Reifman"). This rejection is traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 1-7 are not taught or suggested by Reifman, whether taken individually or in combination any of the other references of record. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw this rejection.

Amendments were made to the claims to more clearly describe features of the present invention. Specifically, amendments were made to the claims to more clearly recite that the present invention is directed to a peer-to-peer communication apparatus and a method for peer-to-peer communication as recited, for example, in independent claims 1 and 6.

The present invention, as recited in claim 1, provides a peer-to-peer communication apparatus for performing one-to-one communication with another communication apparatus via an Internet Protocol (IP) network. The peer-to-peer communication apparatus includes a first means for performing an encryption process and/or an authentication process with respect to a packet. The peer-to-peer communication apparatus also includes a second means for acquiring, from a peer's communication apparatus specified by a user of the peer-to-peer communication apparatus, presence information including information for judging a communication security environment of the peer's communication apparatus and security policy

information including an encryption rule and an authentication rule, each to be applied to packets by the peer's communication apparatus. The peer-to-peer communication apparatus further includes a third means for displaying the presence information and the security policy information, such that the user judges propriety of the security policy information based on the presence information, and for allowing the user to partly change the security policy information. According to the present invention, the first means processes a packet to be transmitted to the peer's communication apparatus in accordance with a security policy approved by the user. The prior art does not disclose all of these features.

As described in the Background of the Invention and the Summary of the Invention, to carry out communication without discarding packets between two communication apparatuses, each having IP security functions, it is necessary for the two communication apparatuses to exchange their respective security policy information showing how each packet is to be encrypted and authenticated, prior to the transmission of the packets. This is necessary so that the packets can be transmitted based on the security policy that satisfies the security requirement placed by the peer's communication apparatus to each other. Further, it is desirable to dynamically change the security level depending on the situation of the communication peer if a security environment changes with the movement of the communication peer as in the case of peer-to-peer communication between mobile terminals.

An object of the present invention is to provide a peer-to-peer communication apparatus capable of relatively freely selecting the security policy in accordance with the current location of a communication peer. The present invention, as claimed, achieves this object.

The above described features of the present invention, as now more clearly recited in the claims, are not taught or suggested by any of the references of record, particularly Reifman, whether taken individually or in combination with any of the other references of record.

Reifman teaches a system and method for facsimile load balancing. However, there is no teaching or suggestion in Reifman of the peer-to-peer communication apparatus or the method for peer-to-peer communication as recited in claims 1 and 6 of the present invention.

Reifman discloses a user interface that simplifies operation of an intelligent facsimile machine (IFAX). In Reifman, a display screen displays a plurality of menus and allows the user to select from the menus. The IFAX can store a plurality of digital cover pages to minimize transmission time for a facsimile cover page. The user may select from a list of stored digital cover pages. The user may also attach a binary data file to a facsimile message and transfer the data to another facsimile machine. The IFAX uses a storage location for storing outgoing facsimile messages. The IFAX periodically check the storage location to determine if more than one facsimile message is to be transmitted to the same location and transmits the facsimile messages in one facsimile telephone call. If the IFAX is coupled to a second IFAX on a network, the two IFAX machines can balance the work load by sending a load transfer request if the number of outgoing facsimile messages exceeds a predetermined threshold level. The IFAX can also route incoming facsimile messages to a variety of destinations such as a floppy disk or other storage device, or an external computer. The IFAX can also relay incoming facsimile messages to another facsimile machine, using a set of relay instructions. The relay instructions may be stored in the IFAX or may be a portion of the incoming

facsimile message. The relay instructions may be nested, and the IFAX sends the facsimile message to a second IFAX with instructions for the second IFAX to relay the facsimile message to a third facsimile machine. The IFAX contains security measures to prevent unauthorized relaying.

One feature of the present invention, as recited in claim 1, and as similarly recited in claim 6, includes a second means for acquiring, from a peer's communication apparatus specified by a user of the peer-to-peer communication apparatus, presence information including information for judging a communication security environment of the peer's communication apparatus and security policy information including an encryption rule and an authentication rule, each to be applied to packets by the peer's communication apparatus. Reifman does not disclose this feature. To support the assertion that Reifman teaches this feature, the Examiner cites column 22, lines 53-55. However, neither the cited text nor any other portion of Reifman teaches or suggest the claimed feature. For example, as described in the cited text, Reifman teaches where the security settings display location 178 shown in the screen display of Fig. 17 allows the user to select options such as data encryption or authentication. The security setting display 178 is provided to the user so that the user can select from any one of processes that the user wants to apply to the facsimile messages. This feature of Reifman is not the same as the claimed feature. For instance, the security setting display 178 does not display encryption or authentication options that were acquired from another facsimile to be a communication peer and does not include "presence information" for judging a communication security environment of the peer's communication apparatus. Furthermore, Reifman does not teach acquiring security policy

information as in the present invention. Accordingly, the present invention is quite different from Reifman.

Another feature of the present invention, as recited in claim 1, and as similarly recited in claim 6, includes a third means for displaying the presence information and the security policy information, such that the user judges propriety of the security policy information based on the presence information, and for allowing the user to partly change the security policy information. According to the present invention, the first means processes a packet to be transmitted to the peer's communication apparatus in accordance with a security policy approved by the user. Reifman does not disclose this feature. To support the assertion that Reifman teaches this feature, the Examiner cites Fig. 20 and column 22, line 55 to column 9. However, neither the cited text nor any other portion of Reifman teaches or suggests the claimed feature. As previously discussed, Reifman does not disclose acquiring presence information including information for judging a communication security environment of the peer's communication apparatus, and further does not disclose acquiring security policy information including an encryption rule and an authentication rule, each to be applied to packets by the peer's communication apparatus. Therefore, it follows that Reifman does not teach or suggest displaying the presence and the security policy information, in the manner claimed.

Therefore, Reifman fails to teach or suggest "second means for acquiring, from a peer's communication apparatus specified by a user of the peer-to-peer communication apparatus, presence information including information for judging a communication security environment of said peer's communication apparatus and security policy information including an encryption rule and an authentication rule,

each to be applied to packets by said peer's communication apparatus" as recited in claim 1, and as similarly recited in claim 6.

Furthermore, Reifman fails to teach or suggest "third means for displaying said presence information and said security policy information such that said user judges propriety of the security policy information based on the presence information, and for allowing the user to partly change the security policy information, wherein said first means processes a packet to be transmitted to said peer's communication apparatus in accordance with a security policy approved by the user" as recited in claim 1, and as similarly recited in claim 6.

Therefore, Reifman does not teach or suggest the features of the present invention, as recited in claims 1-7. Accordingly, reconsideration and withdrawal of the 35 U.S.C. §102(b) rejection of claims 1-7 as being anticipated by Reifman are respectfully requested.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references used in the rejection of claims 1-7.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references used in the rejection of claims 1-7.

In view of the foregoing amendments and remarks, Applicants submit that claims 1-7 are in condition for allowance. Accordingly, early allowance of claims 1-7 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (referencing Attorney Docket No. 520.43249X00).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Donna K. Mason

Donna K. Mason
Registration No. 45,962

DKM/cmd
(703) 684-1120